引用格式：杨晓光，吴杨，张兴伟，等. 构建数智安全新格局 保障新发展格局. 中国科学院院刊，2024, 39(1): 131-142, doi: 10.16418/j.issn.1000-3045.20231207001.
Yang X G, Wu Y, Zhang X W, et al. Building new paradigm of digital intelligence security for new development pattern. Bulletin of Chinese Academy of Sciences, 2024, 39(1): 131-142, doi: 10.16418/j.issn.1000-3045.20231207001. (in Chinese)

构建数智安全新格局 保障新发展格局

杨晓光[1,2]　吴　杨[4]　张兴伟[4]　郑晓龙[3,4*]

1 中国科学院数学与系统科学研究院　北京　100190
2 中国科学院大学　经济与管理学院　北京　100190
3 中国科学院大学　人工智能学院　北京　100190
4 中国科学院自动化研究所　多模态人工智能系统全国重点实验室　北京　100190

摘要　随着党的二十大以后我国进入新发展时代，数智技术的快速发展和广泛应用激活了新一轮经济发展潜力，也给经济社会发展带来了新的安全挑战。文章首先分析了国际与国内新形势下新发展格局的特点，剖析了新发展格局下数智安全风险挑战，涉及微观层面的技术安全、个人安全，以及宏观层面的经济安全、社会安全、文化安全。在此基础之上，文章提出了构建数智安全新格局的基本方法论，给出了一个涵盖数智技术自身安全、保障数智安全的数智技术、数智安全法律法规和政策3个方面数智安全新格局的基本架构。最后，文章探讨了数智安全新格局和新发展格局之间的辩证与螺旋式协同演进关系，为在新的时代保证经济社会的康持续发展提供指导。

关键词　数智安全，数智安全新格局，新发展格局，安全与发展

DOI　10.16418/j.issn.1000-3045.20231207001
CSTR　32128.14.CASbulletin.20231207001

当前，数字技术已经融入社会发展的方方面面，截至2022年底，我国的数字经济规模达到50.2万亿人民币①，占国内生产总值（GDP）比重提升至41.5%，这标志着我国国民经济和社会发展进入了数字化时代。

*通信作者
资助项目：科技创新2030—“新一代人工智能”重大项目（2020AAA0108401），国家自然科学基金（T2293771），国家杰出青年科学基金项目（72225011），中国科学院重大咨询项目（2022-ZW14-Z-027）
修改稿收到日期：2023年12月27日
① 阔步迈向网络强国！8个数字看我国网络基础建设加速度. (2023-07-13)[2023-12-27]. https://www.whb.cn/zhuzhan/sz/20230713/530290.html.

随着大数据、深度学习等人工智能技术的飞速发展，以计算机、信息、通信等为代表的数字技术开始逐步转变为以下一代互联网、生成式人工智能、虚拟现实、数字孪生等为主的数智技术。数据与智能逐渐成为推动社会进步的核心要素，成为经济社会发展的新动力，以及政府和社会治理的新焦点。当下，以ChatGPT为代表的生成式人工智能正在通过大模型赋能引发新一轮智能化浪潮，部分学者认为新一代人工智能的奇点即将到来[1]。然而，在推动技术进步的同时，数智技术的发展也给国家安全体系带来了前所未有的挑战。党的二十大报告对推进国家安全体系和能力现代化、坚决维护国家安全和社会稳定作出战略部署，提出以新安全格局保障新发展格局。在社会形态发生深刻变革的当下，统筹发展与安全无疑是一项复杂的系统工程[2,3]。随着数智技术从多层次的时空尺度上与社会、经济系统的各个功能结构模块产生深度耦合[4]，其引发了数据滥用、算法歧视、就业市场波动等[5]一系列复杂的社会安全治理问题[6]。面对这些困难与挑战，深入剖析数据安全与隐私泄露、算法歧视与不公平性、技术壁垒与数字鸿沟、虚假消息与信息操纵等数智化发展风险的内在机理[7]，全面理解统筹发展和安全的深刻内涵，推进在经济、社会、文化等各个重点领域的数智安全新格局建设，对保障新发展格局至关重要。本文基于总体国家安全观，从新发展格局的国际和国内新特点出发，用微观与宏观视角剖析了新格局下的数智安全风险，提出了构建数智安全新格局的整体框架，并讨论了数智安全新格局和新发展格局的辩证关系，对数智时代的发展与安全的协同提出政策建议。

1 新发展格局的特点

在全面建成小康社会之后，我国开启了全面建设社会主义现代化国家的新征程，形成了新的发展格局。与此同时，在数智技术的推动下，不断深刻变化的国际、国内形势也给当前中国经济社会发展带来了新的挑战。因此，理解当前国际和国内形势之下中国新发展格局所呈现出来的新特点，是构建数智安全新格局的重要前提。

1.1 国际视角

（1）工业革命后，资本主义现代化模式极大地推动了生产力的进步和生活方式的变革。然而，资本主义固有的矛盾也在不断将整个人类的现代化进程推向高度物化和不平衡的困境中。相比之下，中国式现代化道路通过构建人类命运共同体，将本国与世界的现代化发展联系起来，是人类发展模式的创新，将深刻地影响世界现代化进程。

（2）国际上逆全球化趋势加剧，过去几十年形成的全球分工协作局面正在遭到破坏。俄乌冲突、巴以冲突改变着地缘政治局势，给世界前景带来巨大的不确定性。自2017年以来，美国对我国实施多轮制裁，我国亦提出反制措施，双方政治、经贸和安全往来遭遇困难。这些因素从技术、资金、市场等多个角度给我国的外部发展环境带来了严峻的挑战②。

（3）新冠疫情引发需求下降、生产萎缩、贸易受阻、物流中断、失业激增，全球经济陷入衰退的巨大风险之中。为了应对疫情，美国的大规模财政刺激政策加剧了全球通胀，导致美联储开启加息模式，全球资金流动性收紧，进而增加中国企业和政府的外部融资成本。高强度的供给侧冲击直接体现在全球多个国家出现的大面积企业停工停产、职工失业、产业链和供应链大范围中断。2023年8月的调查数据显示：在新冠疫情的影响下，全球失业人数从2019年的1.92亿人飙升到了2020年的2.35亿人。尽管该指标在2022

② 新华社. 形势·态势·大势——2023中国经济首季观察. (2023-04-20)[2023-12-27]. https://www.gov.cn/yaowen/2023-04/20/content_5752288.htm.

年逐步恢复到了2.05亿人，但依然相较疫情前增加了近1 300万的失业人口，且预计2023年还有回升的趋势③。

1.2 国内视角

（1）国内经济由高速增长转向高质量发展。党的十九大报告指出，我国社会主要矛盾已经转化为人民日益增长的美好生活需要和不平衡不充分的发展之间的矛盾。新时代下，经济发展需要从追求数量转向追求更高的质量。在供给端，高质量发展意味着企业需要进行产业体系结构优化，以创新动力实现可持续发展。但这也会使企业在转型过程中面临阵痛和较大的运营压力。在需求端，高质量发展是更平衡、更公平的发展，要求健全分配制度，减小城乡差距、贫富差距，提升人民幸福感[8]。

（2）疫情后国内经济亟待重回正轨。新冠疫情后，叠加错综复杂的国际环境，民众的动机从追求利润最大化转为追求负债最小化，对经济社会发展重回正轨的期盼无比强烈。在这一阶段，保障经济平稳发展，对于民众生活与社会和谐至关重要。

2 新发展格局下的数智安全风险

作为当前先进生产力的代表，数智技术在新发展格局中扮演着极其重要的角色。因此，进一步推进数智技术安全可控的发展对促进经济社会的平稳、高质量发展就显得尤为重要[9]。基于总体国家安全观的理念，笔者将数智安全所涉及的风险分为微观的技术安全、个人安全，以及宏观的经济安全、社会安全、文化安全等5个范畴（图1）。其中，微观安全问题可能随着系统规模的扩大涌现为宏观问题，也可能在传播和反馈的作用下引发级联反应，在短时间内影响到系统的各个方面。

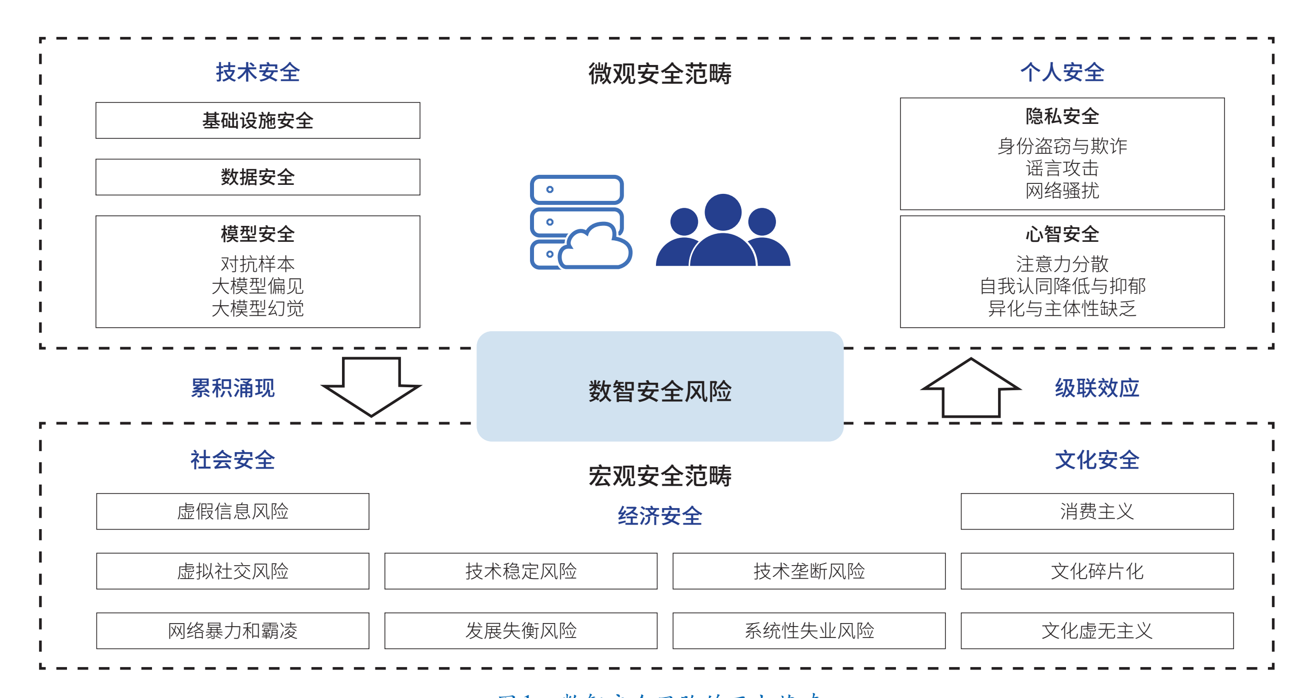


图1 数智安全风险的五大范畴

Figure 1 Five categories of digital and intelligence security risks

③ Number of unemployed persons worldwide from 1991 to 2024. (2023-08-29) [2023-12-27]. https://www.statista.com/statistics/266414/unemployed-persons-worldwide/.

2.1 技术安全

（1）基础设施安全。数智技术的运行需要依赖大量诸如服务器、数据中心和物联网设备等基础设施。如果数据基础设施发生故障、被攻击或遭受灾难，可能导致业务中断、数据丢失、服务不可用，进而带来巨大的经济损失，甚至影响社会的稳定和安全。例如，2022年12月18日，阿里云香港数据中心发生大规模服务中断事件，直接导致澳门金融管理局、众多本地外卖平台及《澳门日报》等传媒应用程序无法使用，对澳门社会层面的平稳运行产生了重大影响。

（2）数据安全。随着科技的发展和人类社会数据量的增加，数据的安全性及泄露风险也越来越受到人们的重视。2005—2022年，美国的数据泄露事件的数目整体呈上升趋势，仅2022年就有1 802起（图2）。在数据存储过程中，黑客攻击或员工疏忽等可能导致客户个人信息、财务记录等敏感数据泄露。在数据使用过程中，员工或其他有权限访问数据的人可能会滥用其权力，将出售敏感数据给竞争对手或非法使用数据。2018年，英国的剑桥分析公司在未经授权的情况下将数百万Facebook（脸书）用户的个人信息用于选民行为分析和推广活动，使得2家公司都面临了严厉的舆论压力、法律调查和监管限制。同年，剑桥分析公司宣布破产[④]。

（3）模型安全。随着深度学习成为人工智能模型的主流，深度神经网络的黑盒性所带来的安全问题逐渐成为人们关注的焦点之一。另外，在ChatGPT等大规模语言模型快速席卷众多行业和深入人们生活的同时，由其产生的错误信息也给这项技术带来了巨大的安全隐患。① 深度学习模型容易受到对抗样本的攻击。这些特殊设计的输入数据可以欺骗模型并导致错误的输出结果，在自动驾驶汽车、医学诊断等场景中

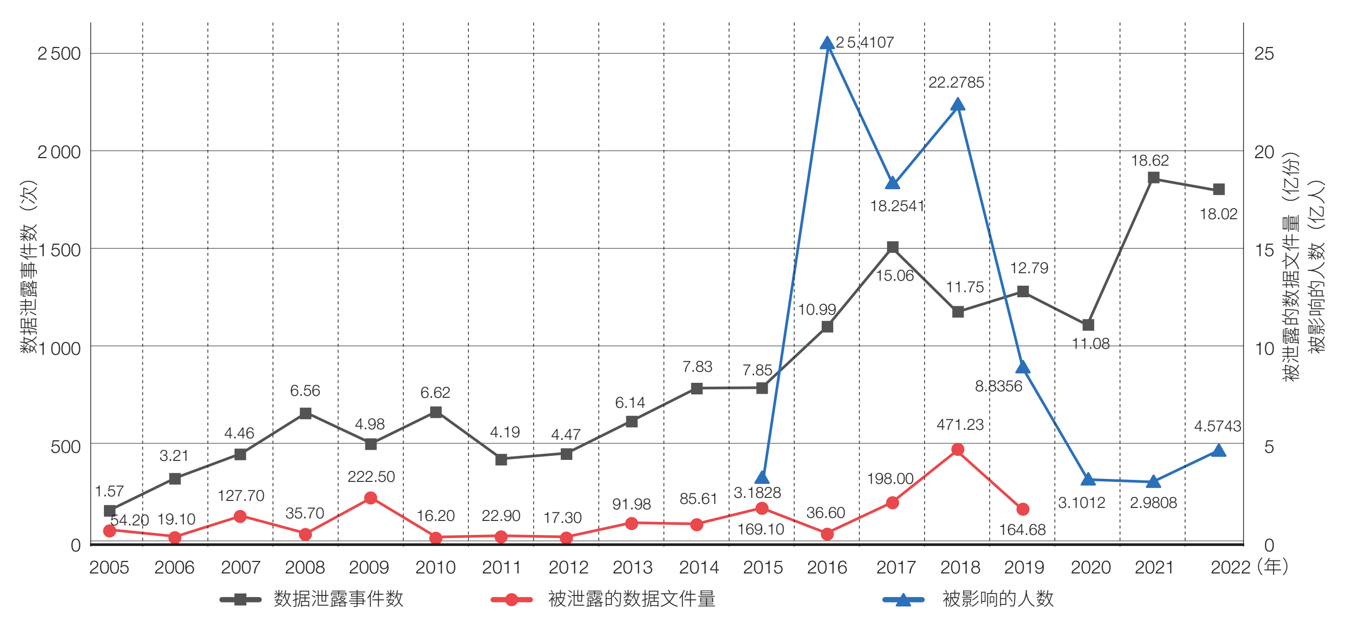


图2　2005—2022年美国数据泄露事件数据

Figure 2　Annual number of data compromises and individuals impacted in the United States from 2005 to 2022

数据来源：Statista数据平台（https://www.statista.com/statistics/273550/）

Data source: Statista (https://www.statista.com/statistics/273550/)

④ Cambridge Analytica. (2023-02-12)[2023-12-27]. https://en.wikipedia.org/wiki/Cambridge_Analytica.

造成严重损失。② 大规模语言模型存在偏见问题⑤。训练方法和数据集的局限性可能导致模型对某些人群或事物表现出不公正或不均衡的行为或决策结果。③ 大规模语言模型存在幻觉问题⑥。在当前大模型生成的文本中，依然存在看似合理但实际上是虚构或错误的信息，这很可能导致使用者产生错误的认知。

2.2 个人安全

（1）隐私安全。隐私安全指的是个体隐私数据泄露时，对其社会生活的危害。泄露的敏感信息（如身份证号、银行账号等）可能导致身份被盗窃、欺诈活动，并带来经济损失。另外，个人信息泄露可能导致谣言、侮辱、骚扰等不良行为，造成精神压力和社交困扰。比如，家庭信息泄露可能导致敲诈勒索和人身安全的威胁。针对英国成年人的调查显示，21%的人担心隐私数据被公司传递给第三方，16%的人担心成为诈骗对象，只有9%的人认为没有必要担心（图3）。同样，在一项2022年针对中国网民的调查中，也有31%的人经常拒绝网站的cookie（浏览活动记录）请求，25.5%的人表示担心科技公司使用自己网上数据的方式（图4）。

（2）心智安全。随着数智技术的发展，人们的精神状态也可能受到环境和技术的影响。例如，社交媒体的过度使用可能导致时间浪费、社交孤立感、焦虑和抑郁等问题；信息过载和注意力分散可能导致注意力不集中、记忆力减退和思维混乱；网络上的匿名性和广泛传播渠道使得欺凌和骚扰行为更加便捷，给受害者带来心理伤害和自尊问题。此外，数智技术还可能造成对人类主体价值、能力、交往方式的异化，剥夺人的选择权利[10]，削弱人的能力[11]，以及引发精神危机和丧失人类尊严，同时也会带来认知极化[12]和各种社交问题。

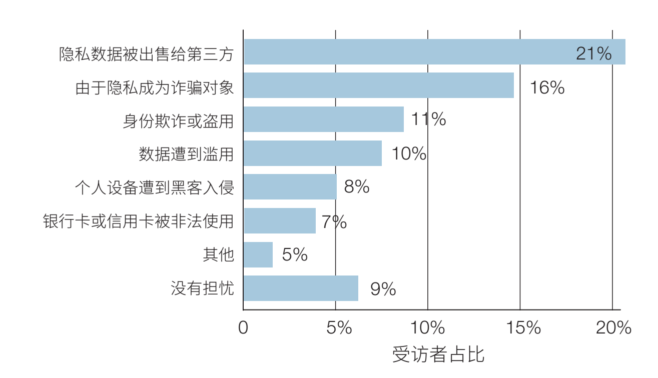


图3 2021年英国公众对于个人隐私安全的担忧

Figure 3 Concerns regarding protection of personal information in UK 2021

数据来源：Statista数据平台（https://www.statista.com/statistics/1184872/）

Data source: Statista (https://www.statista.com/statistics/1184872/)

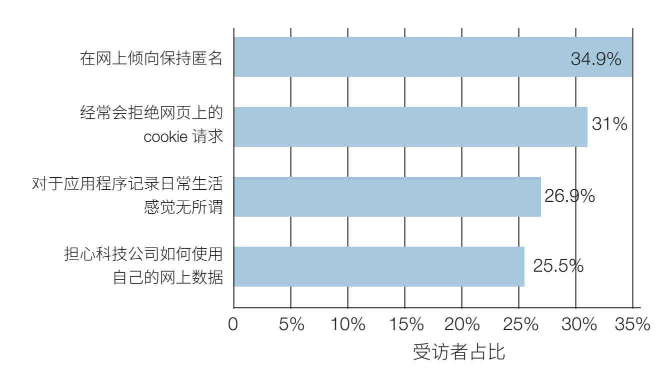


图4 2022年第三季度部分中国网民对于网络隐私和安全的态度

Figure 4 Attitudes relating to online privacy and security among surveyed Internet users in China as of 3rd quarter of 2022

数据来源：Statista数据平台（https://www.statista.com/statistics/1367136/）

Data source: Statista (https://www.statista.com/statistics/1367136/)

2.3 经济安全

（1）技术稳定风险。随着数智技术深入各个经济领域，其微观的技术安全问题可能引发宏观经济系统

⑤ Wu M, Aji A F. Style over substance: Evaluation biases for large language models. (2023-11-12)[2023-12-27]. https://arxiv.org/abs/2307.03025.

⑥ Zhang Y, Li Y, Cui L, et al. Siren's song in the AI ocean: A survey on hallucination in large language models. (2023-09-24)[2023-12-27]. https://arxiv.org/abs/2309.01219.

的风险。无论是金融领域的区块链、智能风控模型，还是制造领域的供应链管理系统出现故障或是受到攻击，都可能会引发级联反应，导致整个交易系统或供应链系统的瘫痪，进而带来巨大的经济损失。

（2）技术垄断风险。当少数大型科技公司垄断了某个智能技术市场时，可能削弱其他创业者和小型企业的竞争力，抑制行业的创新力，阻碍市场的发展和进步。此外，垄断企业所控制的大量用户数据可能侵犯个人隐私权，而公众则缺乏相应的监督和干预手段。

（3）发展失衡风险。在数智化浪潮中，如果某些地区、群体或行业没有抓住先发机遇，就很可能由于缺乏技术能力和资源而滞后于其他地区。研究报告显示，中国东部地区的数字经济发展水平明显领先于中部、西部、东北部，出现了明显的不平衡特征[13]。这种数智技术的不平衡发展与资源、财富、机会的不平衡分配，可能造成经济波动、失业率上升、人口流失、贫富差距扩大等问题，影响社会稳定和谐[14,15]。

（4）系统性失业风险。数智技术的自动化能力使得许多传统劳动任务被机器和软件取代，进而导致制造业、零售业、在线客服、金融服务业、物流行业等传统岗位的大规模失业风险。尽管机器学习工程师、大语言模型的Prompt（提示）工程师等新兴岗位需求会增加，但技术转型过程中工人技能与人力市场需求不匹配和滞后的问题依然可能引起就业市场的阶段性阵痛。

2.4 社会安全

（1）虚假信息风险。互联网和社交媒体的普及极大地提高了人们的每天接收到虚假信息的风险。深度伪造技术（Deepfake）等可以生成高度逼真的换脸图片或视频，然后用于制造政治谣言、虚假新闻或网络欺诈。另外，恶意用户可用ChatGPT等生成式人工智能自动产生大量虚假文本，然后通过机器人账号等手段，用于误导网络社区中用户的价值观。2020年，美国康奈尔大学科学联盟的一项研究显示全球英语媒体发布的3 800余万篇关于疫情的文章中，就有超过110万篇文章包含虚假信息⑦。

（2）虚拟社交风险。随着数智技术深刻重塑当代人的社交方式，社交媒体、即时通信工具等平台使得人们在虚拟空间中随时随地与家人、朋友，甚至全球范围内的陌生人进行交流和互动。然而，过度的虚拟社交除了容易让人沉迷、浪费精力，也可能导致人们面对面的社交互动减少，从而加剧现实中的社交孤独感。同时，一些别有用心的人可以在网络上轻易地隐藏自己的真实身份和发布虚假信息，进而引起误导、欺骗等问题，给他人带来心理上的伤害。

（3）网络暴力和霸凌。数智技术也极大地降低了网络社交中使用辱骂、恶意评论、威胁和歧视性言论等暴力行为的门槛。恶意用户可能通过公开或非法手段获取、发布或散布他人的住址、照片等私人信息，将照片进行篡改甚至淫秽化处理并传播，以侮辱他人。这些行为可能会导致被霸凌对象出现自卑、焦虑、抑郁、自杀倾向等心理问题，也可能让他们在未来的表达过程中选择自我审查或沉默，陷入恶性循环。2021年1月的一项针对2 251位美国成年人的调查发现，41%的受调查用户都亲身经历过某种形式的网络骚扰（图5）。中国社会科学院发布的《2019年中国社会形势分析与预测》（社会蓝皮书）显示：中国青少年在上网过程中遇到过暴力辱骂信息的比例为28.89%。其中，暴力辱骂以“网络嘲笑和讽刺”“辱骂或者用带有侮辱性的词汇”居多，分别为74.71%、77.01%；其次为“恶意图片或者动态图”（53.87%）

⑦ Evanega S, Lynas M, Smolenyak A J. Coronavirus misinformation: quantifying sources and themes in the COVID-19 ‘infodemic’. [2023-12-27]. https://www.researchgate.net/publication/346332946.

和“语言或者文字上的恐吓”（45.49%）⑧。

2.5 文化安全

（1）消费主义。在市场经济高度发达的社会，“消费主义”指的是个人通过购买商品和服务来追求满足感与幸福感的思维方式和态度。基于数智技术的各种便捷购物平台及广告推销算法在降低消费门槛的同时，使得人们的消费决策更容易被操纵和影响，过度关注个人欲望和即时满足，陷入过度消费的陷阱。在这种文化惯性的驱使下，社会资源容易被浪费，个人的幸福感也在永恒的“赚钱—花钱—赚钱”循环中消磨殆尽。有研究针对中国年轻人的消费状态和主观幸福感进行了问卷调查，结果表明：消费主义对出生于1995—2009年的年轻一代的主观幸福感具有显著的抑制作用[16]。

（2）文化碎片化。数智化的推荐系统、个性化定制技术在提高信息搜索效率的同时，也导致个体往往只接受同质化、片面的信息和观点，从而形成所谓的“信息茧房”。“茧房”中的个体反复强化自己的认知，

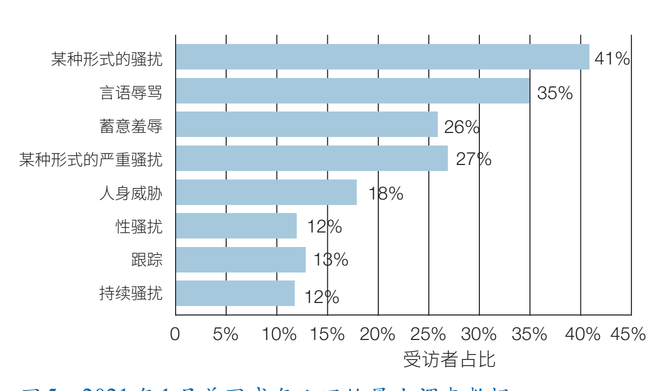


图5　2021年1月美国成年人网络暴力调查数据

Figure 5　Share of adult Internet users in the United States who have personally experienced online harassment as of January 2021

数据来源：Statista数据平台（https://www.statista.com/statistics/333942/）

Data source: Statista (https://www.statista.com/statistics/333942/)

排斥其他观点，形成大量的同质化小型网络社区，产生了大量的亚文化。当不同文化背景的个体在网上碰撞，尤其是涉及言论自由、社会道德、宗教信仰等敏感话题时，就可能引发文化冲突和对立，加剧社会的紧张程度。

（3）文化虚无主义。在新兴的流行文化、工业文化、现代科学实用主义的影响和冲击下，许多传统文化的生存空间受到了挤占，进而产生了文化虚无主义的现象。文化是国家、民族凝聚力的根基。盲目否定自己的文化、历史，会极大地降低人们的集体认同感，进而影响意识形态的稳定性。在数智技术不断加速文化演进的今天，如何在时代的潮流中站稳精神的脚跟，防范文化虚无主义，成为了一个重要命题。

3 构建数智安全新格局

党的二十大报告中强调：“国家安全是民族复兴的根基，社会稳定是国家强盛的前提”。因此，面对数智时代下的各种安全风险，运用系统观念构建数智安全新格局（图6），是保障国家经济社会健康发展和社会平稳运行的必要举措。

3.1 提高数智技术本身的安全

面对数智技术带来的挑战，我们不能盲目拒绝技术进步，而应该尝试提高技术本身的安全性。

（1）加密算法和区块链可以保护信息安全。在信息传输过程中，可以使用DEA（数据加密算法）、RSA等对称或非对称加密算法，以及新兴的基于量子纠缠的通信方式降低数据非法访问、篡改、窃取的风险。区块链技术的去中心化和不可篡改性提高了数字金融交易的可靠性，有助于防范系统性的技术稳定风险。

（2）联邦学习可以保护数据隐私。对于机器学习

⑧ 2019年中国社会形势分析与预测. (2019-01-01)[2023-12-27]. https://www.pishu.com.cn/skwx_ps/bookdetail?SiteID=14&ID=10426484.

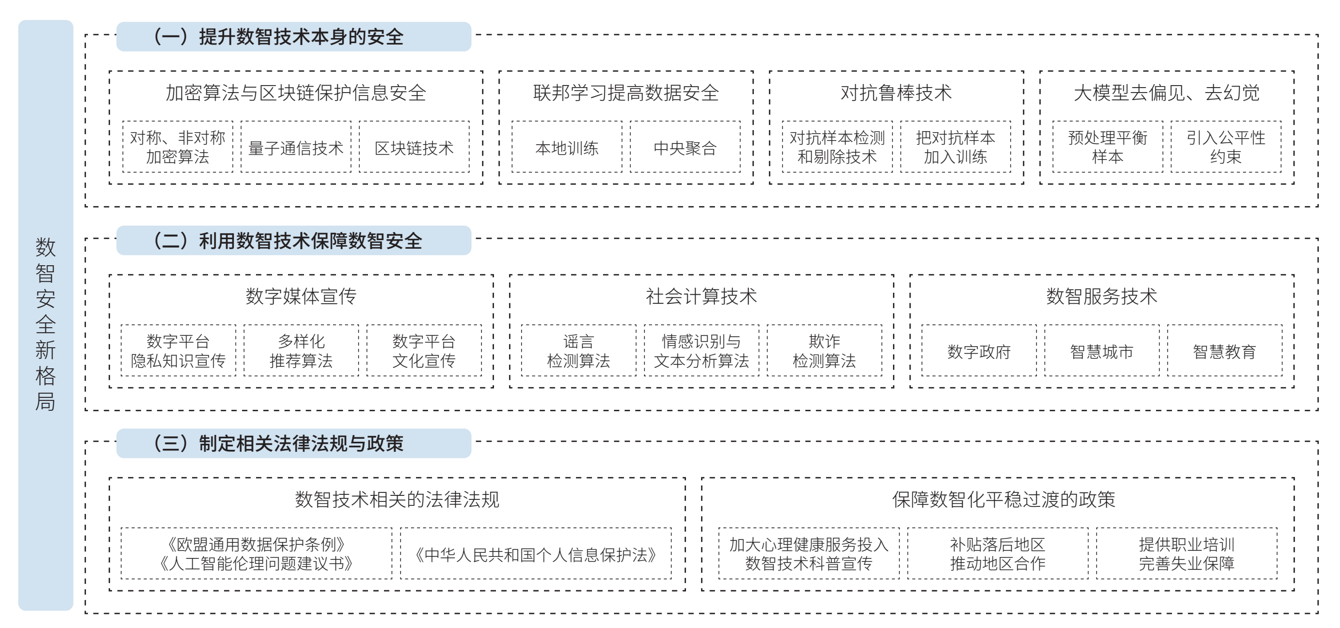


图6　数智安全新格局的基本框架

Figure 6　Basic framework of new paradigm of digital and intelligence security

数据的安全，联邦学习技术[17]提出在多个本地分布式训练模型，然后将参数在中央服务器聚合，以此保障本地数据的隐私性。

（3）对抗鲁棒技术可以提高深度学习模型的可靠性。针对深度学习模型的对抗样本风险，对抗鲁棒技术[18]通过将对抗样本加入训练过程或者设计检测对抗样本的机制，使模型能正确处理被扰动过的对抗样本。

（4）优化训练过程可以缓解大模型的偏见和幻觉问题。通过在训练过程中人为平衡数据集分布，引入公平性约束或额外优化目标，我们能够引导大规模语言模型生成更安全、可靠、多样化的内容，从而避免由于偏见或虚假内容引起的文化冲突。

3.2 利用数智技术保障数智安全

与此同时，也可以运用某些数智技术来解决公共问题、促进个人发展，降低数智技术带来的经济、社会、文化风险。

（1）数字媒体宣传技术可以帮助公众更好地适应数智时代的新变化。例如，相关部门或公益组织可以通过社交媒体分享隐私泄露的实际案例，提高人们的隐私安全意识；通过在推荐系统中引入混合推荐策略，平台能让用户接触到更加多样、异质的内容，从而打破“信息茧房”，优化社区氛围；通过创作更优质的文化作品并加大宣传力度，国家可以促进优秀文化和先进文化的形成，保障传统文化的生存空间，减轻文化虚无主义的危害。

（2）社会计算技术提供了一种自动化防范数智化风险的方案。谣言检测算法⑨可以识别出社交媒体上的虚假信息，帮助平台和相关部门组织谣言的传播，加强社会信任和共识；文本情感识别技术[19]可以帮助网络社区管理者及时发现用户的情绪波动，降低发生网络暴力事件的可能性，对需要帮助的人提供及时的心理干预；欺诈检测算法[20]可以及时检测潜在的诈骗风险，提醒被欺诈者或者帮助警方调查分析。

⑨ Cao J, Guo J, Li X, et al. Automatic rumor detection on microblogs: A survey. (2018-07-10)[2023-12-27]. https://arxiv.org/abs/1807.03505.

（3）数智服务技术能促进社会公平和健康可持续发展。数字政府、智慧城市、智慧教育等数智技术大幅提高了公共服务的效率，促进了社会的公平分配，也能在一定程度上改善地区间数智经济发展不平衡的问题。

3.3 制定数智安全法律法规和政策

（1）相关法律为数智安全提供法理基础。法律法规是维护社会秩序与稳定、保障公民权利与自由、推进社会公正与平等、保障社会安全与公共利益、保障经济社会发展的必要工具，也是推动数智安全建设的重要手段[21]。在国际上，《欧盟通用数据保护条例》（GDPR）针对欧盟成员国的个人数据保护和隐私进行了细化的规定，包括对数据主体的知情权、同意权等。许多国际组织和行业协会也正在积极制定适用于人工智能的伦理准则和行为规范，如联合国教科文组织（UNESCO）的《人工智能伦理问题建议书》等。在国内，2021年通过的《中华人民共和国个人信息保护法》明确了对个人信息的处理原则、个人在信息处理活动中的权利和个人信息处理者的义务，并对个人信息的收集、使用、存储和传输等行为提出明确规定，禁止"大数据杀熟"规范自动化决策，同时加强了相关机构的监管和处罚。

（2）社会政策为数智安全提供实践支持。针对数智化浪潮中个体层面的心智健康问题和社会层面的发展失衡、系统性失业问题，政府可以通过相关的政策来保证社会转变过程的平稳过渡。一方面，政府可以增加心理健康服务的投入、建立心理健康热线、开设心理咨询中心，帮助人们应对智能化浪潮带来的心理压力和问题。另一方面，政府可以通过财政资金的倾斜、给予优惠政策、创立人才培养基地等方法，鼓励相对落后地区加大数字和智能化发展的投入，进而缩小地区之间的发展差距。对于失业人员，政府可以加大对技能培训的投资力度，或者提供更多的创业支持政策，帮助他们顺应智能化时代的新需求。

4 以数智安全新格局保障新发展格局

安全是发展的前提，发展是安全的保障。党的二十大报告中强调："以新安全格局保障新发展格局"。在数智技术推动发展的时代，需要把握好数智安全与经济社会发展之间的辩证关系，以数智安全新格局保障新发展格局。

4.1 数智安全新格局作为新发展格局的保障

数智安全新格局促进经济社会发展的机理可以从保障稳定、刺激创新、加速生产、增强韧性4个维度进行阐述。

（1）保障稳定。数智安全新格局保障了社会和经济系统的长期平稳运行，有助于国家的长远发展和民众生活的安宁和谐。

（2）激发创新。数智安全的需求能激发创新发展能动性，增强公众和企业对政府推动创新的信任，促进多主体参与数智化建设，提高市场活力。

（3）加速生产。数智安全的需求有助于提高全要素生产率增速，通过数智化转型改造基础核心行业和领域，从而推动整个国民经济生产网络的发展。

（4）增强韧性。安全的数智技术为增强产业链韧性提供数据、技术和基础设施支撑，充分利用数据的乘数效应，提升产业链的动态了解和风险应对能力。同时，数智安全新格局的构建还推动了信息通信网络和算力基础设施的发展，为产业的互联网和数字化转型提供坚实基础，确保产业链的自主可控性。

4.2 新发展格局作为数智安全新格局的目的

发展和安全是一体之两翼、驱动之双轮，二者相辅相成、不可偏废。技术的进步和经济社会的发展为数智安全的建设提供了物质基础和手段。

（1）国家需要在安全和创新之间找到平衡。过于强调安全可能抑制创新、限制发展，并带来不良后果。此外，过度关注安全还可能导致资源过度集中在数智安全领域，从而减少在其他领域的投资，进而限

制经济的全面发展。因此，在有限的资源下，国家需要根据风险评估和优先级确定资源的分配。

（2）国家需要动态调整平衡，制定科学合理的安全策略。在实践中，完全消除复杂的社会系统中所有安全隐患是不现实的。因此，在保证基本安全的前提下，国家需要动态调整安全和创新之间的平衡，建立灵活的安全策略和资源分配机制，以面对各种复杂的形势，提升整个社会系统的稳健性。

4.3 数智安全和经济社会发展之间螺旋式的协同演进关系

通过实现数智安全新格局与新发展格局的均衡，安全与发展可以形成一种螺旋式的协同演进关系模式。数智安全的发展需要建立在稳定的经济与社会环境之上，而经济和社会的发展也需要数智技术的支持和保障。在科技与创新的推动下，数智技术的进步可以为社会提供更多的安全保障，如提高技术本身的安全和促进个人发展等；同时，也为经济发展提供了新的机会，推动产业升级和创新。在实现这一目标的过程中，需要关注安全和发展的平衡，避免过度偏重于其中一方而忽视了另一方的重要性。只有通过均衡发展，数智安全新格局和新发展格局才能实现互相促进和共同进步的良性循环。

5 结论与展望

在数智技术的推动下，国际的环境和国内的社会都在经历深刻的结构与功能变化，治理的复杂度也远远超出传统的发展与安全理论的范畴。针对数智技术所带来的新风险，从技术、文化、法律、政策等多角度构造数智安全新格局，对于国家经济稳定发展具有重要意义。在机遇与挑战并存的数智时代，安全和发展应当被视为一个整体。只有正确地平衡、协调安全与发展的关系，才能实现数智时代经济与社会的长期繁荣与稳定。

参考文献

1 Teubner T, Flath C M, Weinhardt C, et al. Welcome to the era of ChatGPT et al.—The prospects of large language models. Business & Information Systems Engineering, 2023, 65(2): 95-101.

2 杨晓光, 高自友, 盛昭瀚, 等. 复杂系统管理是中国特色管理学体系的重要组成部分. 管理世界, 2022, 38(10): 1-24.
Yang X G, Gao Z Y, Sheng Z H, et al. The complex systems management is an important component of the management system with Chinese characteristics. Journal of Management World, 2022, 38(10): 1-24. (in Chinese)

3 王芳, 郭雷. 数字化社会的系统复杂性研究. 管理世界, 2022, 38(9): 208-221.
Wang F, Guo L. Research on system complexity of the digital society. Journal of Management World, 2022, 38(9): 208-221. (in Chinese)

4 陈国青, 曾大军, 卫强, 等. 大数据环境下的决策范式转变与使能创新. 管理世界, 2020, 36(2): 95-105.
Chen G Q, Zeng D J, Wei Q, et al. Transitions of decision-making paradigms and enabled innovations in the context of big data. Management World, 2020, 36(2): 95-105. (in Chinese)

5 杨晓光, 陈凯华, 郑晓龙, 等. 数字技术赋能国家治理现代化建设:挑战及应对. 国家治理, 2023, (5): 52-55.
Yang X G, Chen K H, Zheng X L, et al. Digital technology empowers modernization of state governance: Challenges and countermeasures. Governance, 2023, (5): 52-55. (in Chinese)

6 张权, 雷华美. 互联网平台的社会影响与治理路径. 国家现代化建设研究, 2022, 1(2): 108-123.
Zhang Q, Lei H M. Internet platforms: Social impacts and governance paths. Journal of Modernization Studies, 2022, 1 (2): 108-123. (in Chinese)

7 肖红军. 算法责任:理论证成、全景画像与治理范式. 管理世界, 2022, 38(4): 200-226.
Xiao H J. Algorithmic responsibility: Theoretical justification, panoramic portrait and governance paradigm. Journal of Management World, 2022, 38(4): 200-226. (in Chinese)

8 任保平. 新时代中国经济从高速增长转向高质量发展:理论阐释与实践取向. 学术月刊, 2018, 50(3): 66-74.
Ren B P. Theoretical interpretation and practical orientation of China's economy from high speed growth to high quality development in new era. Academic Monthly, 2018, 50(3): 66-74. (in Chinese)
9 胡洁, 韩一鸣. 政策性开发性金融促进构建双循环新发展格局的机理与路径. 中国发展观察, 2022, (10): 82-86.
Hu J, Han Y M. Mechanism and path of policy-oriented development finance promoting the construction of a new development pattern of double circulation. China Development Observation, 2022, (10): 82-86. (in Chinese)
10 徐源. 马克思"机器论片段"视域下人工智能技术的地方性治理. 山东大学学报(哲学社会科学版), 2022, (5): 145-153.
Xu Y. Local governance of artificial intelligence technology from the perspective of Marx's "Fragment on Machines". Journal of Shandong University (Philosophy and Social Sciences), 2022, (5): 145-153. (in Chinese)
11 徐志向, 罗冬霞. 人工智能促进共同富裕的政治经济学分析. 当代经济研究, 2022, (7): 34-44.
Xu Z X, Luo D X. A political economics analysis of artificial intelligence promoting common prosperity. Contemporary Economic Research, 2022, (7): 34-44. (in Chinese)
12 闫坤如, 曹彦娜. 人工智能时代主体性异化及其消解路径. 华南理工大学学报(社会科学版), 2020, 22(4): 25-32.
Yan K R, Cao Y N. The alienation of subjectivity in the era of artificial intelligence and its solution. Journal of South China University of Technology (Social Sciences Edition), 2020, 22(4): 25-32. (in Chinese)
13 孙小强, 王燕妮, 王玉梅. 中国数字经济发展水平:指标体系、区域差距、时空演化. 大连理工大学学报(社会科学版), 2023, 44(6): 1-10.
Sun X Q, Wang Y N, Wang Y M. China's level of digital economic development: Indicator system, regional disparities, and spatiotemporal evolution. Journal of Dalian University of Technology (Social Sciences), 2023, 44(6): 1-10. (in Chinese)
14 Cattaneo A, Nelson A, McMenomy T. Global mapping of urban-rural catchment areas reveals unequal access to services. PNAS, 2021, 118(2): e2011990118.
15 Jackman J A, Gentile D A, Cho N J, et al. Addressing the digital skills gap for future education. Nature Human Behaviour, 2021, 5: 542-545.
16 田小文, 戴言, 伯乐. "快乐购"且"精致穷":消费主义对Z世代主观幸福感的影响. 消费经济, 2023, 39(4): 81-93.
Tian X W, Dai Y, Bo L. "Pleasant Purchase" while "Exquisite Poverty": A study of the influence of consumerism on generation Z's subjective well-being. Consumer Economics, 2023, 39(4): 81-93. (in Chinese)
17 杨强. AI与数据隐私保护:联邦学习的破解之道. 信息安全研究, 2019, 5(11): 961-965.
Yang Q. AI and data privacy protection: The way to federated learning. Journal of Information Security Research, 2019, 5(11): 961-965. (in Chinese)
18 Zhang X W, Zheng X L, Mao W J. Adversarial perturbation defense on deep neural networks. ACM Computing Surveys, 2021, 54(8): 159.
19 Hakak N M, Mohd M, Kirmani M, et al. Emotion analysis: A survey// 2017 International Conference On Computer, Communications and Electronics (Comptelix). Jaipur: IEEE, 2017: 397-402.
20 Singh Yadav A K, Sora M. Fraud detection in financial statements using text mining methods: A review. IOP Conference Series: Materials Science and Engineering, 2021, 1020(1): 012012.
21 谢琳灿. 欧盟数字立法最新进展及启示. 中国改革, 2022, (6): 79-82.
Xie L C. The development of EU digital legislation and its enlightenment. China Reform, 2022, (6): 79-82. (in Chinese)

Building new paradigm of digital intelligence security for new development pattern

YANG Xiaoguang[1,2] WU Yang[4] ZHANG Xingwei[4] ZHENG Xiaolong[3,4*]

（1 Academy of Mathematics and Systems Science, Chinese Academy of Science, Beijing 100190, China;
2 School of Economics and Management, University of Chinese Academy of Sciences, Beijing 100190, China;
3 School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing 100190, China;
4 State Key Laboratory of Multimodal Artificial Intelligence Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China）

Abstract After the 20th National Congress of the Communist Party of China, China has entered a new era of development. Simultaneously, the rapid advancement and extensive application of artificial intelligent technologies have activated a new wave of economic potential and brought about new security challenges to socioeconomic development. This study firstly analyzes the characteristics of the new development pattern in global contexts, and examines the risks and challenges of digital intelligence security (DIS) under the new pattern, encompassing technological security and personal security at the micro-level, as well as economic security, social security, and cultural security at the macro-level. Based on this analysis, the study proposes the basic methodology for constructing a new paradigm for DIS, which includes enhancing the security of intelligent technology itself, ensuring DIS through intelligent technologies, and establishing relevant legislation, regulations, and policies. Finally, the study explores the dialectical and synergistic relationship between DIS and the new development pattern, providing guidance for ensuring the healthy and sustainable development of social and economic development in the new era.

Keywords digital intelligence security, new paradigm of digital intelligence security, new development pattern, security and development

杨晓光 中国科学院数学与系统科学研究院系统科学研究院研究员。主要研究领域：金融风险管理和公司金融、博弈论与数字经济、社会复杂系统管理等。E-mail: xgyang@iss.ac.cn

YANG Xiaoguang Professor of Academy of Mathematics and Systems Science, Chinese Academy of Sciences (CAS). His research focuses on financial risk management and corporate finance, game theory and digital economy, social complex system management, etc. E-mail: xgyang@iss.ac.cn

郑晓龙 中国科学院自动化研究所研究员。主要研究领域：大数据与社会计算、多模态数据感知与理解、认知图谱与决策智能、社会复杂系统管理等。E-mail: xiaolong.zheng@ia.ac.cn

ZHENG Xiaolong Professor of Institute of Automation, Chinese Academy of Sciences (CAS). His research focuses on big data and social computing, multimodal data perception and understanding, cognitive graphs and decision intelligence, social complex system management, etc. E-mail: xiaolong.zheng@ia.ac.cn

■责任编辑：岳凌生

*Corresponding author